Santa Clara High Technology Law Journal

Volume 12 | Issue 2 Article 5

January 1996

Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet

Jo-Ann M. Adams

COMMENTS

CONTROLLING CYBERSPACE: APPLYING THE COMPUTER FRAUD AND ABUSE ACT TO THE INTERNET*

Jo-Ann M. Adams†

TABLE OF CONTENTS

† B.A., Pomona College; M.A., California State University at Los Angeles; M.B.A., Pacific Lutheran University; J.D., Santa Clara University School of Law, 1996.

INTRODUCTION

Anarchy – is it the ultimate freedom or the ultimate tyranny? As the Internet[1] comes of age, this question surges toward us. In expanding from global village to global metropolis, the Internet has developed its own dark alleys and red light districts. Once a haven exclusively for the military, academicians, and researchers, Internet users now include hackers,[2] thieves, con artists, pedophiles,[3] pornographers,[4] hatemongers, and terrorists.[5]

The scope of computer abuse has far exceeded the bounds originally envisioned by legislators, whose fears included only those of unauthorized access, computer fraud, and alteration of data.[6] Is there an appropriate legislative response that balances freedom from ex-

1. The Internet includes the World Wide Web. The World Wide Web is a portion of the Internet built on hypertext technology. Robert Atkins, *The Art World and I Go On Line*, ART IN AMERICA, Dec. 1995, 58.

2. DENNIS LONGLEY & MICHAEL SHAIN, DICTIONARY OF INFORMATION TECHNOLOGY 146 (2d ed. 1986) (A "hacker . . . [is] a computer enthusiast. The term is normally applied to people who take delight in experimenting with system hardware, software and communication systems. Sometimes used with the connotation of illegality, especially in reference to unauthorized access to data.").

3. WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY OF THE ENGLISH LANGUAGE, UNABRIDGED 1665 (3d ed. 1986) (individuals who have a preference for or addiction to children as the preferred sexual objects); *see* Rob Morse, *Information Highwaymen*, S.F. EXAMINER, Apr. 21, 1994, at A-3.

4. One that produces a depiction of licentiousness and lewdness. WEBSTER'S, *supra* note 3, at 1767.

5. Carolyn Abraham, *Cybercrime: As the Information Highway Grows, So Do the Terrorists, Vandals, Pedophiles and Other Criminals Who Cruise It*, VANCOUVER SUN, Apr. 30, 1994, at B5.

6. Dodd S. Griffith, Note, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453, 455-56 (1990).

ploitation against freedom from government intrusion; individual freedom and creativity against the need to combat increasing crime?

This comment discusses how the Computer Fraud and Abuse Act[7] could be amended to prosecute crimes committed on the Internet. Part I traces the development of the Internet, highlighting its increasingly dark side. It briefly discusses the current struggle between two increasingly polarized camps: those who combat crime and those who defend individual freedom. Part II reviews the evolution of the Computer Fraud and Abuse Act. The impact of the Computer Fraud and Abuse Act on noncomputer crimes is discussed in part III. Part IV discusses proposed amendments to the Computer Fraud and Abuse Act to criminalize the use of protected computers to commit crimes or tortious acts.

I. THE INTERNET

This section describes the development of the Internet and the status of the Internet today. Coinciding with the Internet's growth has been an increase in crimes committed on, or facilitated by, the communication facilities provided by the Internet. Currently there is a struggle between crime control and anarchy in cyberspace. Consequently, many perceive a need for additional legislation.

A. *The Development of the Internet*

The roots of the Internet are grounded in the Department of Defense (DoD). In 1969 the DoD created the Advanced Research Project Agency Network (ARPANET).[8] This network connected DoD computers.[9] At this time only mainframe computers were part of the network, and there were a relatively small number of users.

Through the 1980s, the on-line community grew with the advent of the personal computer. In the mid-1980s, the National Science Foundation established NSF Net to link a small group of supercomputer research centers and researchers at remote academic and governmental institutions.[10] Originally intended as a research tool, the

7. 18 U.S.C.A. § 1030 (West Supp. 1996).

8. Richard Raysman & Peter Brown, *Liability on the Internet*, 3 N.Y.L.J., Nov. 8, 1994, at 3.

9. Gary Anthes, *The History of the Future: As the Arpanet Turns 25, Its Founders Reunite to Talk About the Network That Became the Internet*, COMPUTERWORLD, Oct. 3, 1994, at 101.

10. *Hearing on Internet Access: Subcomm. on Science of the House Committee on Science, Space and Technology*, 103d Cong., 2d Sess. 127 (1994) (statement of Jim Williams, Executive Director, FARNET Inc.) [hereinafter *Hearing on Internet Access*]. *See also* Raysman & Brown, *supra* note 8.

federal government encouraged universities and research institutions to use the NSF Net. Connecting the universities turned out to be an investment. The universities responded by making significant software contributions, including:

a) Berkeley UNIX (operating system) by University of California (Berkeley);
b) Mosaic interface (multi-media interface for information retrieval) and Eudora (e-mail) by University of Illinois;
c) Gopher (information retrieval tool) by University of Minnesota;
d) Pine (e-mail) by University of Washington; and
e) CU-SeeMe (low-cost video conferencing) by Cornell.[11]

The NSF originally discouraged commercial traffic.[12] However, by the mid-1980s the Commercial Internet Xchange (CIX)[13] circumvented these restrictions. Midlevel networks leased data circuits wholesale from telephone companies and provided them to institutions on a fixed cost basis.[14] In addition, government contributed an estimated twelve million dollars in annual subsidies to NSF.[15]

The number of computers at each node[16] and the number of network nodes continued to expand. Over time the network became a network between networks, or the Internet.

B. *The Internet Today*

To fully appreciate the legal complexities of regulating the Internet, one must first understand the magnitude of the Internet. The Internet has an estimated fifteen to twenty-five million users[17] in ninety-two countries[18] and is growing at the rate of five to eight percent per month.[19]

Originally designed to connect the disparate computers of the DoD, connectivity[20] still remains the Internet's most unique aspect.[21]

---

11. *Hearing on Internet Access, supra* note 10, at 129.
12. Raysman & Brown, *supra* note 8.
13. Peter H. Lewis, *Internet for Profit; Businesses Rush to Capitalize on the Internet*, 14 No. 11 COMPUTER SHOPPER, Nov. 1994, at 178.
14. *Hearing on Internet Access, supra* note 10.
15. Raysman & Brown, *supra* note 8.
16. LONGLEY & SHAIN, *supra* note 2, at 234 (a node is "a point of interconnection to a network.").
17. Graeme Browning, *Net Effects*, NAT'L. J., June 3, 1995, § Communications.
18. *Internet Crime Soars*, INFO. WK., Oct. 10, 1994, at 20.
19. Joe Clark, *The Online Universe: Find Out Why Some 30 Million People Count Themselves as Citizens of this Mysterious World*, TORONTO STAR, Oct. 20, 1994, at J1.
20. FRANK J. GALLAND, DICTIONARY OF COMPUTING: DATA COMMUNICATIONS, HARDWARE AND SOFTWARE BASICS, DIGITAL ELECTRONICS 50 (1982) ("the ease or practicality of connecting functional units").

It features a common telecommunications protocol (TCP/IP),[22] which is now used by most of the computers in the world.[23]

The most highly-used services offered by the Internet can be grouped into four categories:

1) fast-changing information: news, sports scores, financial services;

2) electronic communications: e-mail, real-time conversations, conferencing;

3) transactional services: banking, shopping travel reservations; and

4) entertainment: games, horoscopes, movie reviews.[24]

Current Internet connectivity providers can also be grouped into four categories:

1) Mom and Pop shops: small businesses, usually with one location;

2) Regionals: typically nonprofit, university affiliated, subsidized by the National Science Foundation (NSF);

3) National Independents: for-profit entities, nationwide or international services;

4) The Big Guys: IXCS,[25] RBOCs,[26] and Cable TV operators.[27]

When the seeds of the Internet were planted, no one expected its explosive growth – least of all its developers. Developer Severo Ornstein's initial reaction to DoD's request for proposals was: "Sure we could build such a thing, but I don't see why anybody would want it."[28]

The Internet's rapid acceptance was undoubtedly fueled by an exponential drop in the cost of delivery. In 1987 the cost per

---

21. Arman Danesh, *Servers Are Display of Confidence in Internet*, SOUTH CHINA MORNING POST, Oct. 4, 1994, at 5A.

22. Terminal Control Program/Internet Protocol. MARK S. MERKOW, BREAKING THROUGH TECHNICAL JARGON: A DICTIONARY OF COMPUTER AND AUTOMATION ACRONYMS 132 (1990).

23. Katie Hafner, *Profile; For 'Father of the Internet,' New Goals, Same Energy*, N.Y. TIMES, Sept. 25, 1994, § 3, at 4.

24. Raysman & Brown, *supra* note 8.

25. Interexchange channels. JERRY M. ROSENBERG, MCGRAW-HILL DICTIONARY OF INFORMATION TECHNOLOGY AND COMPUTER ACRONYMS, INITIALS, AND ABBREVIATIONS 88 (1992) (for example, AT&T, MCI, Sprint).

26. Regional Bell Operating Companies. *Id.* at 149 (the regional telephone companies created after the breakup of AT&T).

27. *Hearing on Internet Access*, *supra* note 10, at 119 (statement of William L. Schrader, Chairman, President, and CEO, Performance Systems International Inc.).

28. Anthes, *supra* note 9.

megabyte[29] (MB) was ten dollars. Two years later that figure dropped to one dollar. By 1993 it had dropped again to thirteen cents.[30]

C. *Anarchy on the Internet*

Fearing that the network would be vulnerable to attack, the ARPANET, the Internet's predecessor, was intentionally designed with no central authority.[31] NSF Net continued that philosophy. This lack of control caused one reporter in Britain to comment:

> [D]espite its size, Internet is not actually owned or controlled by anyone. Its roots lie in liberal US academic institutions, and freedom of speech and an 'anything goes' credo are important parts of the Internet ethos.[32]

While the FCC says it has authority to regulate public computer networks, it has not yet exercised any control over the Internet.[33] Consequently, no central regulatory body governs the Internet. The one guiding force, the NSF, is withdrawing from active participation as the Internet evolves commercially.[34]

Most Internet users enjoy the anarchy of the Internet. For example, Eric Schmidt, Chief Technology Officer of Sun Microsystems, has great hope in the free-wheeling nature of the Internet, which he likens to the Wild West.[35] He welcomes the commercialization of the Internet and feels that it will contribute to its breadth.[36]

In testifying before the House Subcommittee on Science, William L. Schrader, Chairman, President, and CEO of Performance Systems International, Inc., echoed these sentiments. Schrader feels that commercial providers continually improve the quality of the Internet. Like Schmidt, Schrader welcomes the commercialization of the Internet.[37]

Despite the optimism in the commercial sector, the federal government is well aware that there is a growing dark side to the Internet.

---

29. JERRY M. ROSENBERG, DICTIONARY OF COMPUTERS, INFORMATION PROCESSING, AND TELECOMMUNICATIONS 375 (1987) (roughly one million bytes of information; a byte holds one character, such as, A, B, C, #, &).

30. *Hearing on Internet Access, supra* note 10, at 129.

31. Raysman & Brown, *supra* note 8.

32. Malcolm Wheatley, *Auntie Ventures into Taboo Zone*, INDEPENDENT, July 31, 1994, at 12.

33. Brad Patten, *Sex Rides the Fast Lane on Info Superhighway*, PHOENIX GAZETTE, Feb. 7, 1994, at C1.

34. Raysman & Brown, *supra* note 8.

35. WEBSTER'S, *supra* note 3, at 2616 (The western United States in its frontier period).

36. Danesh, *supra* note 21.

37. *Hearing on Internet Access, supra* note 10 (statement of William L. Schrader, Chairman, President, and CEO of Performance Systems International, Inc.).

D. *Crimes on the Internet*

Crimes perpetrated on the Internet can be grouped into three major categories: 1) computer crimes, 2) fraud, and 3) noncomputer crimes. Computer crimes include those crimes where knowledge of a computer system is essential to commit the crime. Fraud comprises its own category, since it was the only noncomputer crime acknowledged by the Computer Fraud and Abuse Act of 1986. Noncomputer crimes include all other forms of crime.

1. Computer crimes

Computer crimes typically include hacking,[38] worms,[39] and viruses.[40] Hackers divide themselves into two groups: 1) hackers, who have no intent to do "any criminal activity,"[41] and 2) crackers[42] who intend to engage in criminal activity.[43] Reports show that the number of incidents of electronic break-ins into computer systems has nearly doubled each year. At the Carnegie Mellon University in Pittsburgh, the Computer Emergency Response Team (CERT) notes an increase in reported incidents.

Year	Number of Break-Ins[44]
1989	132
1990	252
1991	406
1992	773
1993	1,334
1994	2,341

The Department of Energy also noticed that the number of electronic break-ins has more than doubled each year. In 1990 there were

38. Laura Evenson & Michelle Quinn, *Outlaws on the Cyberprairie*, S.F. CHRON., Apr. 2, 1995, at 1/Z1 (Hacking is computer trespass. There may, or may not, be any intent to engage in any other criminal activity.).

39. Unites States v. Morris, 928 F.2d 504, 505 n.1 (2d Cir. 1991) (Worms are computer programs that migrate from computer to computer without attaching to the computer's operating system.).

40. *Id.* (Viruses are computer programs that migrate from computer to computer and attach to the computer's operating system.).

41. Evenson & Quinn, *supra* note 38 (Hackers do not consider breaking into a computer system a crime.).

42. *Id.* (Crackers: CRiminal hACKERS).

43. *Id.*

44. *Hacker 'Not Very Difficult to Catch,'* USA TODAY, Feb. 20, 1995, at 3B.

forty-five electronic break-ins into Department of Energy Computers; in 1993 there were four hundred electronic break-ins.[45]

At first seen as a prank by young kids, law enforcement is now taking computer crimes very seriously – both here and abroad. People have come to realize that hacking is not victimless. Recently a hacker passed through the network belonging to The Boeing Company. The Boeing Company paid $75,000 to its employees to have them check their system and verify that no damage was done.[46] CERT observed that hackers are increasingly sophisticated.[47] While ten years ago most hackers were youthful pranksters interested in demonstrating technical prowess, many Internet users today feel that more sinister forces are at work – a sort of net mafia.[48] For example, in early February 1994, CERT concluded that there was an organized effort to infiltrate the Internet.[49]

The hacker may go beyond breaking into a computer system and actually alter or destroy data.[50] This damage is usually done by either

---

45. *Science & Technology Week: Computer Police Strike Back Against Internet Crimes*, (CNN television broadcast, April 2, 1994) [hereinafter *Computer Police*].

46. Evenson & Quinn, *supra* note 38.

47. Joshua Cooper Ramo, *A SWAT Team in Cyberspace*, NEWSWEEK, Feb. 21, 1994, at 73.

48. *Id.*

49. *Id.*

50. Several individuals have been indicted for computer crimes. *See* David Johnston, *Cracking Down on Cybercrime*, OTTAWA CITIZEN, June 18, 1995, at A5 (A 20-year old man in Toronto charged with accessing nearly every university in Ontario); Richard Karpinski, *Accused Hackers Plead Guilty*, TELEPHONY, July 16, 1990, at 12 (Robert Riggs, Adam E. Grant, and Franklin E. Darden, Jr., members of the Legion of Doom, pled guilty to conspiracy to defraud Bell South); Evenson & Quinn, *supra* note 38 (Kevin Poulson used knowledge of the phone system to win two Porsches and $50,000 in cash from various Los Angeles radio stations; Justin Tanner Petersen was Poulson's accomplice in the radio scams and pled guilty to tapping credit card information bureau and transferring $150,000 from a Glendale financial institution; Mitnick stole credit card numbers from network computers and hacked computers at MCI Communications and Digital Equipment Corporation and destroyed accounting files); John Markoff, *Case Stirs More Fear of Hackers; Internet Showing Its Vulnerability*, HOUS. CHRON., Feb. 17, 1995, § A at 19; John Johnson, *A Computer Terrorist or a Prankster?*, L.A. TIMES, February 26, 1995, § Metro, Part B, at 1(Mitnick stole secret computer files from various companies); Caroline A. Duffy, *Crackdown in Cyberspace? Boston University Student Indicted for Criminal Activity on Internet*, PC WK. Apr. 18, 1994, at 15 (David LaMacchia, an MIT student, was indicted for setting up a computer to download copyrighted software worth more than $1 million); Mark Guidera, *Internet Falls Prey to Crime; Cyber Crooks Put Users on Defensive*, PHOENIX GAZETTE, Aug. 12, 1994, at A27 (Clarkson University had at least one confirmed case of destroying and possibly stealing files. In researching the break-in, Clarkson employees found evidence that as many as twenty other universities may have been targeted as well); Laurent Belsie, *The Dark Side of Cyberspace*, CHRISTIAN SCI. MONITOR, July 18, 1994, at 119 (Paul Bedworth broke into approximately 10,000 computer systems in the United States, France, Germany, India, and Russia); *Computer Police*, *supra* note 45 (Mark Abene broke into computer networks used by the government, many banks and phone companies); Paola Piglia & A.J.S. Rayl, *Secrets of the Cyberculture; Counterculture Movement Lead by Computer Hackers*, 15 OMNI 58 (Nov. 1992),

viruses or worms.[51] Viruses and worms cause havoc by deleting files, by replicating until all space is used and the system crashes, or by bringing the system down.[52]

2. Fraud

Fraud was the only noncomputer crime recognized in the Computer Fraud and Abuse Act of 1986.[53] Therefore, fraud could be seen as the keystone between computer crimes and noncomputer crimes. Internet fraud includes: stealing credit card numbers, transferring funds to a numbered account in another country, ordering goods and then cancelling the charge to the bank account.[54] To identify credit card numbers, hackers use software known as packet sniffers.[55]

Computer networks have also been used to perpetrate investment fraud.[56] Typically these schemes lure naive consumers to invest in future technologies. While the future technologies may have been legitimate, the investment opportunity was a scam.[57] Other schemes have included unregistered securities, Ponzi scams,[58] pyramid

available in LEXIS, NEWS Library, ARCNWS file (Robert T. Morris, Jr. released a worm that infected U.S. 6,500 computers on the Internet, which caused $150 - 200 million in damages).

51. *Terms to Know*, INFOWORLD, Feb 13, 1995, at 91.

52. *Id.*

53. 18 U.S.C. § 1030.

54. Joseph Radigan, *Info Highway Robbers Try Cracking the Vault . . . Or 50 Million Ways to Fleece Your Banker*, U.S. BANKER, May 1995, at 67. *See also* Amy Cortese, *Warding Off the Cyberspace Invaders*, BUS. WK., Mar. 13, 1995, at 92 (an MCI technician was charged with capturing more than 50,000 credit card numbers; he sold these cards to a network of dealers, resulting in fraudulent charges in excess of $50 million); Guidera, *supra* note 50, at A27 (an international ring operating in Europe used stolen telephone calling card numbers to call the United States and set up Internet accounts; they paid for the accounts using the stolen credit cards); *Cyberblotter: The Internet's Most Wanted*, PITTSBURGH POST-GAZETTE, July 25, 1995, at C4 (two seemingly legitimate vendors bilked $27,000 from Internet users by offering trading cards for a popular game called "Magic"; a 15-year old boy stole a credit card number from the Internet and bought a $4,800 computer to be delivered to Arnold Ziffel of Green Acres fame); John Larrabee, *Cyberspace a New Beat for Police*, USA TODAY, April 26, 1994, at 1A (John Lucich, investigator with the New Jersey Attorney General, accessed a dozen underground computer bulletin board services (BBSs) where stolen credit card numbers were swapped among computer hackers).

55. Packet sniffers scan the content of Internet messages looking for 16-digits broken up by spaces (the format for charge cards). Charles Arthur, *Crime Gangs Use Internet to Access Credit Card Fraud*, INDEPENDENT, June 2, 1995, § Home, at 3.

56. L.A. Lorek, *Fraud Entering Cyberspace; High-tech Con Artists Ply Schemes via Information Avenues*, SUN-SENTINEL, July 3, 1994, at 1G.

57. One company used a thirty-minute infomercial to bilk $16.5 million from 1,600 investors for specialized mobile radio licenses. Other con artists pitch wireless cable television franchises; one firm collected $10.3 million from 740 investors. *Id.*

58. Mark Simon, *No Assets Found At Loan Firm; San Jose Company Being Investigated for Scam*, S.F. CHRON., Feb. 1, 1995, at A15 ("A Ponzi scam is a pyramid scheme in which phony investment are sold and the money is paid out to earlier investors to create the appearance of legitimacy.").

schemes,[59] and stock manipulation plans.[60] Despite these risks, there are at least forty to fifty financial institutions who have set up programs on the Internet.

3. Noncomputer Crime

The most recent and most disturbing trend has been the use of the Internet to perpetrate traditional, noncomputer crimes. The most widely reported crimes are: 1) distribution of pornography, 2) pedophilia,[61] 3) stalking, and 4) hate speech. Other crimes include death threats, bomb manufacturing instructions, and virtual gambling casinos.[62]

a. Pornography

The use of the Internet to distribute pornography has received much media attention.[63] Pornographic images are loaded onto the Internet. The Internet user must access files and download them to view the images. The vast majority of pornographic images are kept in private bulletin board services, which usually require you to aver that you are at least eighteen years of age.

Estimates of the amount of pornography available on the Internet vary widely.[64] A Carnegie-Mellon University study indicated that more than eighty-three percent of all images stores in Usenet news groups are pornographic and nearly fifty percent of all downloads from commercial bulletin boards depict child pornography, incest, tor-

59. WEBSTER'S, *supra* note 3, at 1852 (the series of operations involved in enlarging one's holdings "by using paper profits as margin to buy additional amounts").

60. Lorek, *supra* note 56, at 1G.

61. WEBSTER'S, *supra* note 3, at 1665 (sexual perversion in which children are the preferred sexual object).

62. Ron Bartlett, *Global Casinos Pose Virtual Mess*, TAMPA TRIB., Aug. 27, 1995, at 1.

63. For example, on LEXIS when searching for "Internet and pornography," in 1994 there are nearly 300 newspaper articles, in 1995 there were nearly 2,000, and in the first six weeks of 1996, there were over 500. LEXIS, NEWS library, PAPERS file.

64. In the first half of 1994 alone there were several incidents of child pornography reported using computer networks. *See* Charlotte Parsons, *Cheap Price Techno Porn Back on Sale*, SOUTH CHINA MORNING POST, Apr. 24, 1994, at 3 (U.S. law enforcement officials uncovered a child computer pornography ring centered at Birmingham University in Britain); John Larrabee, *Cyberspace a New Beat for Police*, USA TODAY, Apr. 26, 1994, at 1A (In Medford, Massachusetts police entered the home of a rape suspect and found computers, camera equipment, high-resolution video monitors. Police suspect that the man operated a network that transmitted child pornography); Barbara Kantrowitz, et al., *Child Abuse in Cyberspace*, NEWSWEEK, Apr. 18, 1994, at 40 (United States Customs Service seized computers and discs of 88 Americans downloading child pornography from Denmark); Michael Da, *New Moral Crisis: Computer Porn*, HOUSTON POST, Feb. 20, 1994, at A10 (a college computer instructor in Farmington, Connecticut traded pornographic pictures of children through a secret BBS; an Abilene man became the first person convicted by a federal jury of importing illegal child pornography by computer).

ture, or mutilation.[65] This translates to more than 450,000 pornographic images and text files, which were accessed more than six million times.[66] There is currently no way of knowing how may of these six million accesses were made by children.

Critics of the study, however, point out that this study was limited to the Usenet groups and included private-adult-bulletin-board systems, which are not publicly available. Therefore, this grossly exaggerates the amount of pornography available to children on the Internet.[67] Moreover, it has been reported that children not only access pornography, they distribute it.[68]

The amount of pornography placed on the Internet in the United States may drop precipitously, however, now that a Milpitas, California couple was convicted[69] in Tennessee on eleven counts of obscenity. They face fifty-five years in prison and a $2.75 million fine.[70]

b. Pedophilia

A second example of noncomputer crime is pedophilia. Many bulletin boards on the Internet deal with sex. In fact, of the top ten BBSs, several are exclusively for sex talk.[71] The vast majority target adults. However, others target children. For example, one BBS in Ottawa, The Boywatchers Inc.,[72] is a forum for pedophilia.[73]

Pedophilia and stalking are found in both the public and private areas of the Internet. Most contact with children takes place in publicly-available chat rooms. Chat rooms are areas in cyberspace wherein individuals can engage in real-time interactive conversations.

---

65. Dan Coats, *'Dark Side' of the Internet*, WASH. POST, June 30, 1995, at A23.

66. Joe Chidley, *Red-Light District*, MACLEAN'S, May 22, 1995, at 58.

67. Professors Donna Hoffman and Thomas Novak of Vanderbilt University state that Rimm's statistics are misleading. For example, of the 14,000 electronic news groups worldwide, only 200 carry pornographic messages or pictures. This represents less than one-half of one percent of all messages on the Internet. Scott L. Powers, *Cyberporn has Time up in Flames*, B. GLOBE, July 19, 1995, at 67; Elizabeth Corcoran, *Cybersensitivity? Critics Say the Media Overreacted to a Study on Computer Pornography*, WASH. POST, June 28, 1995, at C1, C8.

68. In 1993, police in Winnipeg and Toronto raided a BBS which distributed obscene material; a 14-year-old boy allegedly operated the service. Abraham, *supra* note 5, at B5. In Sacramento County, a 14-year-old boy was brought in by his mother with a handful of floppy disks containing pornographic materials, which he had received from an adult on-line. Kantrowitz, *supra* note 64.

69. United States v. Thomas, 74 F.3d 701 (6th Cir. 1996).

70. James C. Harrington, *Should the Plug be Pulled on Cyberporn? Beware of Chilling Freedom of Expression*, DALLAS MORNING NEWS, Apr. 9, 1995, at 1J.

71. Abraham, *supra* note 5.

72. "Inc." means incest rather than "incorporated." Kevin O'Brien, *Down a Dark Alley*, PLAIN DEALER, May 22, 1994, at 1C.

73. Abraham, *supra* note 5.

Far more frightening than access to pornography in cyberspace is the harm done to children in the real world as the result of contacts made in cyberspace. Children have been lured from their homes and molested based on conversations in chat rooms on the Internet.[74]

c. *Stalking*

Another problem prevalent on the Internet is the increased use of computerized data bases for stalking. The ratio of men to women on the Internet is three to one. Many women become victims of on-line harassment, or stalking, and receive obscene and/or misogynist[75] mail from e-perverts.[76] For example, Cheryl L. Willis was barraged by mail from a man called "Hellraiser" who tried to sabotage her system. He even sent nasty messages to her friends.[77] Connecticut Representative Patricia Dillon, a daily Internet user, drafted legislation after learning that a woman received repeated threatening messages. The messages falsely accused the woman of being promiscuous and ridiculed her retarded son.[78]

Jake Baker, a student at the University of Michigan (UM), was arrested for stalking when he placed three stories on the Internet about fantasies that included, rape, mutilation, torture, and murder.[79] Jake

---

74. *See* Vincent J. Schodolski, *Online Anonymity Conducive to Vice; Teens are Vulnerable in Cyberspace*, CHI. TRIB., June 11, 1995, § News, at 19 (A 13-year-old girl left home to accept an offer from a man to run around a room naked all day and all night; she has not been seen since. John Rex is accused of kidnapping and raping two boys he met through a computer bulletin board service. Alan Paul Barlow was convicted for describing his sexual fantasies to 14-year-old girls in Montana and New Jersey); Mary Murphy, *Computer Prowlers Stalk Kids*, ORLANDO SENTINEL, July 9, 1995, at 1 (Prosecutors were able to convict Barlow after he solicited lewd photographs and sent them Polaroid cameras. Donald Harvey sent explicit e-mail messages and pictures, and then he flew to Orlando to have sex with what he thought was a 14-year-old boy); Larrabee, *supra* note 54 (Michael Austin, who has a history of sexual assaults, used his computer to befriend boys, lured them into meeting him, and raped at least two of the boys. Austin is currently serving a 20-year prison sentence); Kantrowitz et al., *supra* note 64, at 40 (A computer engineer used America Online to communicate with a 14-year old boy and arranged to meet him in person. Before taking the boy home, he handcuffed, shackled, and blindfolded him. Once home, he spanked him with a belt, forced him to have an enema, shaved his legs, and pubic hair, and engaged him in oral and anal sex. He then ordered boy to write about the abuse online; the father discovered the graphic account); Sandy Rovner, *Molesting Children by Computer*, WASH. POST, Aug. 2, 1994, at Z15 (A 14-year-old girl thought she was corresponding with a teenage boy. She gave him her phone number. She began receiving indecent phone calls from a 51-year-old man).

75. WEBSTER'S, *supra* note 3, at 1444 (one given to a hatred of women).

76. Rovner, *supra* note 74.

77. Jonathan Rabinovitz, *Rules of Road on the Information Highway: Law Makes Harassing by Computer a Crime*, N.Y. TIMES, June 13, 1995, at B4.

78. *Id.*

79. Philip Elmer-DeWitt, *Snuff Porn on the Net: A Student's Sex Fantasies Raise Disturbing Questions About the Limits of Free Speech in Cyberspace*, TIME, Feb. 20, 1995, at 69.

used the name of a fellow student as the victim's name and sent e-mail to someone in Canada expressing that he would like to carry out these fantasies. The FBI arrested Jake under a federal statute that prohibits interstate transmission of a threat to kidnap or injure. U.S. District Judge Avern Cohn threw out the five-count indictment holding that you cannot be arrested for your fantasies.[80]

While the number of incidents are few, it will be interesting to watch the development in this area. Will jurisdictions follow Rep. Dillon's lead, or will jurisdictions treat Internet stalking as fantasy?

d. Hate speech

Lastly, the Internet has been used for hatemongering.[81] This includes jokes about, threats to, and advice on how to kill members of minority groups. Right-wing extremists from militia members to Aryan Nation hatemongers are using the Internet to spread their message.[82] Since Neo-Nazis are barred from selling their books in Germany, they have turned to the Internet to distribute their hate tracts.[83] To date, no cases involving hate speech on the Internet have been prosecuted.

e. Other crimes

There are numerous other crimes that people have engaged in through the use of the Internet. For example, in Laval, Quebec three boys were maimed after using instructions on how to build a pipe bomb, which they had acquired from a nineteen year-old Massachusetts man.[84] A nineteen year-old Texas College student was indicted for sending death threats to President Clinton by e-mail.[85] Cybergambling is a rapidly developing market as offshore companies, based mostly in the Caribbean, offering virtual reality casinos.[86]

As the Internet becomes more widely used, the frequency and variety of noncomputer crime has increased. This has resulted in some legislators calling for regulation of cyberspace.

---

80. United States v. Baker, 890 F.Supp. 1375 (E.D. Mich. 1995).

81. Abraham, *supra* note 5.

82. David Willman & Ralph Frammolino, *Facing the Fear of an Enemy from Within*, L.A. TIMES, Apr. 22, 1995, at A1.

83. Belsie, *supra* note 50.

84. Abraham, *supra* note 5.

85. Larrabee, *supra* note 54.

86. Ron Bartlett, *Global Casinos Pose Virtual Mess*, TAMPA TRIB., Aug. 27, 1995, at Florida/Metro 1.

E. *Struggle within the Anarchy: Combatting Crime versus Individual Freedom*

With Internet crime increasing, battle lines are being drawn. As system administrators and law enforcement officials scan bulletin boards, posing as victims and tracing transactions, they meet a wave of resistance from Internet operators and users who deplore government snooping and intrusion. Users fear that the Internet, or portions of it, will be shut down or censored in the name of law and order.

1. Combating Crime

Combatting crime on the Internet is still in its infancy. However, there are three major groups making efforts to control cyberspace: the Computer Emergency Response Team, major providers of commercial on-line services, and law enforcement officials.

To combat unauthorized access on the Internet, any break-ins are reported to the Computer Emergency Response Team (CERT) located at the Carnegie-Mellon University in Pittsburgh.[87] A staff of 15 programmers do the initial investigation. Complicated security breaches are farmed out to an unofficial brain trust.[88]

To combat pornography and indecency, some major commercial services, such as Prodigy and America Online, censor sex talk.[89] However, efforts to screen content may markedly decrease as operators face possible liability for obscenity. In *Stratton Oakmont Inc. v. Prodigy Services Co.*[90] Judge Ain ruled that Prodigy was a publisher, not merely a conduit or library, in a libel case. Judge Ain ruled that because Prodigy monitors content it can be held liable for slanderous material.[91] This ruling will undoubtedly discourage commercial services from monitoring content of transmissions.

Specially trained law enforcement officials, or those with computer backgrounds, hack into secret bulletin boards.[92] Many times they try to locate suspects by posing as women or teen-age boys (the most likely victims).[93] By posing as women or teen-age boys, law

87. Guidera, *supra* note 50.

88. Joshua C. Ramo, *How to Fight Crime on the Internet*, NEWSWEEK, Feb. 21, 1994, at 73.

89. Michelle Slatalla, *Prodigy Libel Ruling Changes Online Scene*, NEWSDAY, May 28, 1995, at 4.

90. 23 Media L. Rep. 1794 (Sup. Ct. N.Y. 1995), *available on* LEXIS, 1995 N.Y. Misc. LEXIS 229 (N.Y. Sup. 1995).

91. Clinton Wilder, *Prodigy Put on the Line – Service May Be Held Liable for Content*, INFORMATIONWEEK, June 12, 1995, at 24.

92. Larrabee, *supra* note 54.

93. *Id.*

enforcement officers engage in conversation and eventually set up a sting operation.

Some law enforcement officials formed their own groups. In the United States the Hi-Tech Crime Network is an informal group of computer-savvy police officers.[94]

Not only do law enforcement officials try to capture criminals on-line, they have started to solicit help from Internet users. For example, the FBI's UNABOM Task force was the first probe in which federal agents used the Internet to solicit help from Internet users.[95] The Task Force was investigating a series of mail bombings during the past fifteen years that killed three and injured twenty-three – the bomber is referred to as the UNABOMBER.[96] Scholars and researchers were targeted to receive these explosive devices. As part of their investigation, the FBI kept a page on World Wide Web of the status of the case.

2. Individual Freedom

While the FBI states that e-mail transmissions have the same privacy rights as surface mail,[97] many civil libertarians remain skeptical. Some doubt they will continue to enjoy the freedom they currently have on Internet. The Electronic Frontier Foundation, for example, is dedicated to preserving individual liberties on the Internet. Mike Godwin, a lawyer for the Foundation says:

> I hear "pedophile" every time they try to justify some new intrusion. . . . There's nothing inappropriate about law enforcement policing cyberspace, but I'm skeptical of all their claims. There aren't enough pedophiles in the country to justify all the hype.[98]

Many people liken the Internet to the telephone system. One observer noted:

> [W]e do not have laws saying who can or cannot drive down the street or use the telephone, and no one has charged the local phone company when a scam artist uses a telephone to cheat some elderly couple out of their savings. . . . The same should go for the Internet

---

94. *Id.*

95. Bill Wallace, *Computer Net Used to Solicit Bombing Clues*, S.F. CHRON., Dec. 31, 1993, at A1.

96. John O'Brien, *Technology Fights Back Against Unabomber*, CHI. TRIB., Aug. 13, 1995, at C1.

97. Rovner, *supra* note 74.

98. Larrabee, *supra* note 54.

> and online services. It should be open for anyone and everyone to use.[99]

The recent Memphis case convicting Robert and Carleen Thomas of eleven counts of distributing pornography was particularly disturbing to Internet users and operators.[100] The Thomases were convicted based on the "contemporary community standards" of Memphis, Tennessee.[101] This decision will probably be appealed to the United States Supreme Court where the Court may use it as an opportunity to redefine the notion of community standards.[102] However, one observer at the Thomas trial felt that the many of the 20,000 digital images would have offended any community, because they included images of incest, bestiality, genital torture, urine and feces.[103]

Operators and users found this decision a disturbing form of censorship, because it applied Memphis, Tennessee standards of obscenity to material produced in Milpitas, California and distributed internationally.[104] Many feel that it sets a dangerous precedent. Bruce Kramer, ACLU attorney in a "Deep Throat" case,[105] commented on the recent conviction of the Thomases: "The message going out there is, do this at your peril . . . . This is censorship any way you look at it."[106]

The conviction of the Thomases "hit the on-line community like a cold shower."[107] Laura Brito operates a Missouri BBS called Laura's Lair. She is also the co-administrator of an adult BBS network called Throbnet. Commenting on the Memphis decisions, Brito said: "Everybody is scared . . . . We wish we knew what the rules are. If I knew what the rules are, I certainly would follow them."[108] However, complying with community standards everywhere may be difficult, if not impossible.

---

99. James Crawley, *Memphis Porn Decision is Far-Reaching: Ruling Causes Concerns About Right of Online Computer Users*, SAN DIEGO UNION-TRIB., Aug., 16, 1994, at 9.

100. United States v. Thomas, 74 F.3d 701 (6th Cir. 1996).

101. *Id.* at 710-11.

102. *Id.*

103. Jim McMahon, *Cyberporn Can Be Regulated*, S.F. EXAMINER, Aug. 21, 1994, at B-5.

104. David Landis, *Sex, Laws & Cyberspace; Regulating Porn: Does it Compute*, USA TODAY, Aug. 9, 1994, at 1D.

105. In the "Deep Throat" cases the U.S. attorney's office in Memphis charged 60 people and companies for transporting *Deep Throat* across state lines even though the film was never shown in Memphis. Joshua Quittner, *Computers in the '90's; Life in Cyberspace; The Issue of Porn on Computers*, NEWSDAY, Aug. 16, 1994, at B27. *See* United States v. Battista, 646 F.2d 237 (6th Cir. 1981), *cert. denied*, 454 U.S. 1046 (1981); United States v. Peraino, 645 F.2d 548 (6th Cir. 1981).

106. Quittner, *supra* note 105.

107. Landis, *supra* note 104.

108. *Id.*

The latest complication in Internet telecommunications is that foreign governments are exerting pressure on service providers to censor the content or prevent access to certain material. Germany first targeted sex-related news forums and persuaded CompuServe to cut off access.[109] German law enforcement also investigated anti-Semitic and neo-Nazi propaganda.[110]

In typical Internet style, when the German government threatened to cut off the site at Web Communication in Santa Cruz, California, free-speech advocates in other parts of the country copied the material and posted it on their web sites.[111]

F. *The Need for Legislation*

While several groups are dedicated to maintaining the unbridled freedom of the Internet, Congress has realized the need for legislation. One of the prime reasons for legislation is to address the concerns Brito expressed: define the rules so that people will know how to conform their behavior. What should be the appropriate governmental response is sporadically debated. It includes such diametrically-opposed suggestions as "don't regulate it, because technology moves too fast for Congress to respond"[112] to "allow common law to regulate technology, because common law moves so slowly."[113] Others have postulated that any form of regulation is inappropriate for cyberspace, particularly regulating concepts of property and copyright.[114] One observer suggested denying copyright privileges to pornography and letting economics drive pornographers out of business.[115] Another suggested that pornography is just a phase, and the Internet will grow through it.[116]

However, it is clear that the information industry has reached the critical mass necessary to detonate government regulation:

---

109. Peter Lewis, *Blocking the Net Easier Said Than Done*, DENV. POST, Jan. 28, 1996, at H-24.

110. Ernst Zundel, a German living in Canada, placed on the Internet propaganda denying the Holocaust. Hiawatha Bray, *UMass Shuts Down Web Site Containing Neo-Nazi Material; Student Intended Protest of German Censorship*, B. GLOBE, Feb. 2, 1996, at 28.

111. *Id.*

112. John Frohnmayer, *Don't Tread on the 'Net*, PITTSBURGH POST-GAZETTE, Apr. 9, 1995, at F1.

113. *Id.*

114. *Cruising the Information Highway: Cyberspace and the American Dream; A Magna Carta for the Knowledge Age*, ETHNIC NEWSWATCH, Mar. 31, 1995, at 42.

115. Casey B. Mulligan, *Pornography, Profits and the Internet*, CHI. TRIB. June 28, 1995, Perspective, at 19.

116. Tim Jackson, *The Porn Brokers*, IRISH TIMES, June 19, 1995, at 8.

> The revolution has only just begun, but already it's starting to overwhelm us. It's outstripping our capacity to cope, antiquating our laws, transforming our mores, reshuffling our economy, reordering our priorities, redefining our workplaces, [and] putting our Constitution to the fire.[117]

As a result, national politics is polarizing into two camps: those whose interests remain with the Industrial Age and those whose interests are hooked to the emerging Digital Age. This is creating stranger-than-usual bedfellows, such as the right-wing libertarians and counterculture hippies who hold as core values more self-reliance and less governmental intrusion.[118]

II. THE COMPUTER FRAUD AND ABUSE ACT (18 U.S.C. § 1030)[119]

In response to the demand for regulating the Internet, Congress should use The Computer Fraud and Abuse Act as its vehicle. The Internet has already been deemed to fall within the purview of the Act as evidenced by the conviction of Robert Morris in 1988.[120] The Act, which currently limits its scope to computer crimes and fraud, could be expanded to include noncomputer crimes. The scope of the Act has been continuously broadened as the scope of computer crime broadens.

At the time Congress passed the Computer Fraud and Abuse Act of 1984, the computer industry did not know the scope of computer crime.[121] However, Congress knew that over twenty states had already enacted legislation in this area and many more were in the process of enacting computer legislation.[122] This part discusses the evolution of the Computer Fraud and Abuse Act from its inception through the most recent proposed amendment in 1995.

A. *The Computer Fraud and Abuse Act of 1984*

In enacting the Computer Fraud and Abuse Act of 1984, Congress rejected broader bills that would have tied the criminalization to interstate commerce. Congress intentionally limited the scope of the legislation to protect only the vital federal interests.[123] In passing the

---

117. Steven Levy, *TechnoMania*, NEWSWEEK, Feb. 27, 1995, at 24.

118. Peter Leyden, *Politics of the Digital Age Creating Stranger-Than-Usual Bedfellows*, STAR TRIB., June 25, 1995, at 2T.

119. 18 U.S.C.A. § 1030 (West Supp. 1996).

120. United States v. Morris, 928 F.2d 504, (2d Cir. 1991), *cert. denied*, 502 U.S. 817 (1991). *See infra*, note 168 and accompanying text.

121. Griffith, *supra* note 6, at 455-56.

122. *Id.* at 459.

123. *Id.* at 456.

Computer Fraud and Abuse Act, Congress was restrained by two fears: redundancy[124] and overreaching.[125]

Consequently, to narrow the scope, scienter[126] was required for each of the offenses to the extent that the person had to knowingly access "the computer without authorization, or having accessed a computer with authorization, used the opportunity such access provided for purposes to which such authorization did not extend."[127] In addition, the original act covered only three narrow areas: 1) accessing a computer to get classified defense or foreign relations information to harm the United States or to advantage a foreign nation, 2) accessing a computer to get financial records from a financial institution or consumer information from consumer reporting agencies, and 3) modifying, destroying, or disclosing information if such conduct affects the government's use of the computer.[128]

In subsection (a)(1) Congress intentionally excluded the inadvertent access by a government employee into unauthorized files. This section is directed to those outside the government. However, it also includes those within the government who exceed their authority. As one of the three original provisions of the bill, Congress narrowly drew this section to only include the most vital federal interests.

Subsection (a)(2) targets computer hackers and other criminals accessing financial information without authorization. Congress intentionally drafted the intent requirement to exclude information incidentally obtained or information obtained legitimately. The intent requirement applies only to the access prong of the subsection. Therefore, a prosecutor must prove intent to access – not intent to injure.[129]

The scope of subsection (a)(3) is limited by the phrase "affects the use of the Government's operation of such computer." It required the prosecutor to prove that the access affected computer operation. If the access did not affect computer operation, subsection (a)(3) does not apply.[130]

The offenses defined in subsection (a) are criminalized in subsection (b); subsection (c) sets out the penalties. Subsection (c) differen-

---

124. An unnecessary repetition of federal legislation when the states already have passed legislation on the subject matter.

125. When federal authority stretches into areas and preempts where the states already have legislated; Griffith, *supra* note 6, 458.

126. BARRON'S LAW DICTIONARY 433 (3d ed. 1991) ("Previous knowledge of an operative state of facts.").

127. 18 U.S.C. § 1030(a)(1)-(3) (1988).

128. *Id.*

129. Griffith, *supra* note 6, at 463-464.

130. *Id.*

tiates first offenses from subsequent offenses and gives much stiffer penalties for subsequent offenses. A subsequent offense is defined as "a conviction for another offense under such subsection or an attempt to commit an offense punishable under this subparagraph."[131]

B. *Criticism of the 1984 Act*

Legislators realized that the 1984 Act was only a first step toward controlling computer fraud and abuse and that the legislation was incomplete. Critics of the 1984 Act noted that the scienter requirement was higher than required for other applicable espionage laws.[132] Subsection (a)(2) on the protection of financial and credit information was too limited. First, it protected a very narrow class of financial and credit information. For example, it excluded the bank's deposits in other institutions and loan records. Second, it protected only individuals and not corporations.[133] Subsection (a)(3) on modifying, destroying, or disclosing information required that prosecutors prove the additional elements of modification, destruction, or disclosure.[134] Both subsections (a)(2) and (a)(3) had a drafting inconsistency that resulted in a use exemption: if a person with authority accessed information for which they were not authorized, there were no sanctions for using the data. This was clearly inconsistent with Congressional intent.[135]

C. *The Computer Fraud and Abuse Act of 1986*

In response to these criticisms, and in light of suggestions to increase the scope of the legislation, the Computer Fraud and Abuse Act was amended in 1986.

The 1986 Amendment made significant changes to the Act. Prior to the 1986 amendment, the Act defined the intent requirement as "having accessed a computer with authorization." The 1986 amendment simplified this awkward phrase to read "exceeds authorized access." The 1986 Amendment also defined the key terms used in the original Act.[136] By making access alone a criminal offense, the 1986 Amendment transformed subsection (a)(3) into a strict trespass provision.[137] However, this section limited the trespass offense to those offenders who were not employed by the federal government and had

131. 18 U.S.C. § 1030(c). For a detailed discussion of the penalties, see *infra* part II.F.
132. Griffith, *supra* note 6, at 467.
133. *Id.* at 467.
134. *Id.* at 468.
135. *Id.* at 464.
136. 18 U.S.C. § 1030(e).
137. *Id.* § 1030(a)(3). *See* Griffith, *supra* note 6, at 476.

no authority to access a federal interest computer.[138] Congress had a potential concern that the word "disclosure" in subsection (a)(3) might discourage those seeking to expose wrongdoing by the federal government. Therefore, the 1986 Amendment deleted the word "disclosure."[139] In response the concerns expressed by the Department of Justice, the 1986 Amendment reduced the intent requirement of sections (a)(2) and (a)(3) from "knowingly" to "intentionally." This brought the intent requirement in line with those for espionage.[140] The House Report on the Criminal Code expressed a fear that a knowing standard imposes liability on inadvertent access.[141] Therefore, legislators substituted an intentional standard to target those who intentionally, rather than inadvertently, access files without authorization.[142] Finally, the 1986 Amendment repealed the specific fines in the original act and replaced them with the fines imposed "under this title."[143] This, in effect, tied the crimes to the Criminal Fine Enforcement Act of 1984.[144]

In addition, three new offenses were added: subsection (a)(4) – access with intent to defraud; subsection (a)(5) – altering, damaging or destroying data or preventing authorized use; subsection (a)(6) – access with intent to defraud traffics in any password.[145]

Subsection (a)(4) created a federal computer fraud offense. Congress intentionally decided not to pattern this section after the mail and wire fraud statutes.[146] Unlike the mail and wire fraud statutes, the computer must be an integral part of the fraud and may not be wholly extraneous. Congress did not want to punish mere access of a computer at or near the time of the fraud. Congress also emphasized theft of property to be sure that the defendant intended to or did obtain something of value and not just computer time.[147]

Subsection (a)(5) primarily targets: 1) losses greater than $1,000 during a single year, and 2) alteration data for medical treatment. Since this offense is a felony, a $1,000 threshold was set to exclude minor amounts or cases in which the amount of loss could not be proven. However, losses can easily reach this threshold because losses include the following expenses: lost computer time, reprogram-

138. Griffith, *supra* note 6, at 476.
139. *Id.* at 474.
140. *Id.*
141. H.R. REP. No. 1396, 96th Cong., 2nd Sess. (1980)
142. Griffith, *supra* note 6, at 475-76.
143. 18 U.S.C. § 1030(c).
144. 18 U.S.C. § 3623; Griffith, *supra* note 6, at 481.
145. 18 U.S.C. § 1030(a)(4)-(6).
146. S. REP. No. 432, 99th Cong., 2nd Sess. (1986), at 9.
147. *Id.* at 9-10; 18 U.S.C. § 1030(a)(4).

ming, restoring data, certain network communication fees, and the time of authorized users who rely on the altered data.[148]

The prosecutor need not show pecuniary loss for altering records involved in medical treatment.[149] Congress felt that tampering with medical records is serious enough to be a felony.[150]

Subsection (a)(6), the last of the new offenses of the 1986 amendment, criminalizes the trafficking of computer passwords. This subsection targets hackers trading computer passwords over bulletin boards. The mental requirement includes both "knowingly" and "with intent to defraud."[151] It applies to passwords or information that allow access to federal government computers. However, this section also includes password trafficking if it affects interstate or foreign commerce.[152]

One of the major enhancements to the 1986 version of the Act was the definition of key terms in subsection (e). At the suggestion of the Justice Department,[153] Congress expanded the definition of "Federal interest computer" to include "a computer . . . which is one of two or more computers used in committing the offense, not all of which are located in the same State."[154] This addition covered those cases in which state law enforcement officials lacked jurisdiction. If a crime defined in the Act was committed using computers in more than one state, local law enforcement officials now had recourse at the federal level.

D. *Expanding the Scope of the Act: the 1988, 1989, and 1990 Amendments*

The Computer Fraud and Abuse Act[155] was originally proposed to be very narrow in scope. In the ensuing years the rate and seriousness of computer fraud and abuse grew rapidly. As a result, the Computer Fraud and Abuse Act has been amended several times. The 1988 Amendment corrected the punctuation in Subsection (a)(2), clarifying that the Act covers all financial institutions and not just those that issue credit cards. The 1989 Amendments replaced "a bank" with "an institution" in Subsection (e)(4)(a), and struck out: "an institution with accounts insured by the Federal Savings and Loan Insur-

148. Griffith, *supra* note 6, at 480.
149. *Id.* at 479-80.
150. S. REP. No. 432, 99th Cong., 2nd Sess. (1986), at 9.
151. 18 U.S.C. §1030(a)(6).
152. *Id.* § 1030(a)(6)(A).
153. Griffith, *supra* note 6, at 481-82.
154. 18 U.S.C. §1030(e).
155. *Id.* § 1030.

ance Corporation."[156] Consequently, any institutions with deposits insured by the FDIC are now included. The 1990 Amendments corrected the reference to paragraph "r" in the Atomic Energy Act of 1954 to paragraph "y"[157] and added "commonwealth" to the definition of "State."

The 1990 Amendments also expanded the scope of the act to include two additional "financial institutions" in subsection (e)(4):

> (H) a branch[158] or agency[159] of a foreign bank[160] (as such terms are defined in paragraphs (1) and (3) of section 1 (b) of the International Banking Act of 1978);
> (I) an organization operating under section 25[161] or section 25(a)[162] of the Federal Reserve Act.

E. *The 1994 Amendment*

The 1994 Amendment rewrote the fifth offense: altering, damaging, or destroying data, or preventing authorized use of the computer. This amendment created two offenses based on intent. Subsection (A) covers intentional acts; subsection (B) covers reckless acts. Once the requisite mens rea[163] is defined, the wording within each section is identical. In summary, the section proscribes: 1) damaging or potentially damaging a computer system or its components, and 2) withholding, denying, or causing the withholding or denial of use of a computer system or its components. These acts must be without au-

---

156. *See* 18 U.S.C.A. § 1030(e)(4)(A) (West Supp. 1996) (history of the amendments to the Computer Fraud and Abuse Act).

157. Paragraph y defines the term "restricted data" includes "all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy." 42 U.S.C. § 2014(y).

158. "'[B]ranch' means any office or place of business of a foreign bank located in any State of the United States at which deposits are received." 32 U.S.C. § 3101(3).

159. "'[A]gency' means any office or place of business of a foreign bank located in any State of the United States at which credit balances are maintained incidental to or arising out of the exercise of banking powers, checks are paid, or money is lent but at which deposits may not be accepted from citizens or residents of the United States." 32 U.S.C. § 3101(1).

160. "'[F]oreign bank' means any company organized under the law of a foreign country . . . For the purposes of this act the term "foreign bank" includes, without limitation, foreign commercial banks, foreign merchant banks and other foreign institutions that engage in banking activities usual in connection with the business of banking in the countries where such foreign institutions are organized or operating." 32 U.S.C. § 3101(7).

161. "Any national banking association possessing a capital and surplus of $1,000,000 or more" which is accepted by the Board of Governors of the Federal Reserve System. 12 U.S.C. § 601.

162. "Corporations to be organized for the purpose of engaging in international or foreign financial operations." 12 U.S.C. § 611.

163. The mental state accompanying a forbidden act. STEVEN H. GIFIS, LAW DICTIONARY 296 (1991).

thorization and must either cause loss of more than $1,000 in any one-year period or alter medical records.

F. *Penalties*

Subsection (c) sets out the penalties for each of the six offenses. The text of the punishments for all six offenses are similarly worded. The table below summarizes these punishments. In the 1986 Amendment all fines were described as "a fine under this title," which tied them to the Criminal Fine Enforcement Act of 1984.[164] The Criminal Fine Enforcement Act allows for fines up to $100,000 for misdemeanors and $250,000 for felony convictions.

Penalties under 18 U.S.C. § 1030

Section	First Offense	Subsequent Offense
(a)(1): Access with Intent to Injure the US	Fine or prison for not more than 10 years	Fine or prison for not more than 20 years
(a)(2): Access to Financial Records	Fine or prison for not more than 1 year	Fine or prison for not more than 10 years
(a)(3): Access which Affects Use	Fine or prison for not more than 1 year	Fine or prison for not more than 10 years
(a)(4): Access with Intent to Defraud	Fine or prison for not more than 5 years	Fine or prison for not more than 10 years
(a)(5)(A): Intentional Altering, Damaging or Destroying Data or Preventing Authorized Use	Fine or prison for not more than 5 years	Fine or prison for not more than 10 years
(a)(6): Access with Intent to Defraud Traffics in Passwords	Fine or prison for not more than 1 year	Fine or prison for not more than 10 years

G. *Cases Prosecuted under the Act*

Because of the severe limitations of the 1984 Act, the federal government never prosecuted any cases under it. Critics correctly

164. 18 U.S.C. § 3623; Griffith, *supra* note 6, at 481.

noted that an Act cannot have a deterrent effect if prosecutions are never brought.

Since the Act was revised in 1986, several cases have been prosecuted under the various subsections of Title 18 U.S.C. § 1030. Of the cases pursued, most involved theft or fraud including loss of property.[165]

One case, *United States v. Rice*,[166] involved fraud with no pecuniary loss. This case involved unauthorized access and unauthorized disclosure of confidential information. An IRS agent, Rice, knew that his long-time friend was under investigation for drug dealing, including the possible forfeiture of his house. At his friend's request, Rice checked the IRS computer to see if his friend was being investigated by the IRS. Since Rice was not a member of the criminal division, he exceeded his authorized access. Rice also went to the IRS investigator to see what the codes on the printout meant. He then told his friend the meaning of the codes and the investigator's name. This case was brought under 18 U.S.C. § 1030(a)(3). Rice was convicted (by a jury) of computer fraud for accessing the computer system of a government agency without authority; his convictions were affirmed.[167]

Another case, *United States v. Morris*,[168] involved pecuniary loss but not fraud. Morris was a first-year graduate student at Cornell University working toward his Ph.D. in computer science. For an assignment he developed a worm to demonstrate the inadequacies of current security measures on computer networks. The assignment required the worm to occupy little space while using minimal computer time and not interfering with normal use. Morris included a feature to determine if the worm had already infected the computer. If the worm had infected the computer, the worm would not replicate.

---

165. *See* United States v. Sykes, 4 F.3d 697, 698 (8th Cir. 1993) (unauthorized use of an automated teller machine and personal identification number); United States v. DeMonte, 1992 U.S.App. LEXIS 11392 (6th Cir. May 12, 1992) (*per curiam*) (*aff'd* in part, *rev'd* in part, and remanded, 25 F.3d 343 (6th Cir. 1994) (an employee made more than 50 fictitious computer entries defrauding the VA of more than $46,000 and during the investigation admitted that he had earlier defrauded the VA of $30,000); United States v. Coleman, 1991 U.S. App. LEXIS 14833, at *2 (9th Cir. July 3, 1991) (attempt to defraud the government of $9,469,348 by cashing fraudulent government check); United States v. Carron, 1991 U.S. App. LEXIS 4838 (9th Cir. May 20, 1991) (unauthorized computer access using two credit cards); United States v. Lewis, 872 F.2d 1030 (6th Cir. 1989) (embezzled approximately $47,000 from AmeriTrust, a federally insured bank); United States v. Fernandez, 1993 U.S. Dist. LEXIS 3590, at *3 (S.D.N.Y. Mar. 25, 1993) (various computer-related crimes, including accessing a federal-interest computer without authorization and altering or damaging information).

166. United States v. Rice, 1992 U.S. App. LEXIS 9562 (4th Cir. May 4, 1992).

167. *Id.* at *5.

168. United States v. Morris, 928 F.2d 504, (2d Cir. 1991), *cert. denied*, 502 U.S. 817 (1991).

Up to this point Morris' potential liability was limited to unauthorized access. However, Morris also wanted to make sure that programmers at the target sites did not kill the worm. Therefore, he programmed the worm to duplicate itself every seventh time it determined that the target computer was already infected. Morris released the worm onto the Internet where it spread and multiplied; it eventually caused computers at various educational institutions and military sites to crash. The federal government convicted Morris under 18 U.S.C. § 1030(a)(5).[169]

III. THE COMPUTER FRAUD AND ABUSE ACT AND NONCOMPUTER CRIMES ON THE INTERNET

The first three offenses of the Computer Fraud and Abuse Act have extremely limited, if any, applicability to Internet users in the business, academic, or personal arena. They are part of the original act, which Congress intentionally drew with a very narrow scope. The last three offenses have greater applicability as the scope of the Act expanded with the 1986 Amendments.

A. *Unauthorized Access to National Defense, Foreign Relations, or Restricted Data*

The first offense covers unauthorized access to national defense, foreign relations, or other restricted data as defined in the Atomic Energy Act.[170] Congress obviously drew this subsection very narrowly. It covers only information that must be protected for reasons of national defense, foreign relation, or selected information of the Atomic Energy Act.

To prevail under this section, the prosecutor must prove unauthorized access (or access exceeding authorization) and intent or reason to believe that such information is to be used to the injury of the United States, or the advantage of any foreign nation. Consequently, if Internet users access corporate or academic files without authorization, this section would not apply unless the prosecutor proved that the hacker intended (or there was reason to believe) that the information obtained was to be used to injure the United States or to the advantage any foreign nation. This subsection provides no protection to commercial, academic, or personally-owned computers unless the computers are used in work regarding national defense, foreign relations, or the Atomic Energy Act.

169. 928 F.2d at 511.

170. 42 U.S.C. § 2104(y); 18 U.S.C. § 1030(a)(1) (1988).

B. *Unauthorized Access to Financial Records*

The second offense covers unauthorized access to financial records of financial institutions, card issuers, or consumer reporting agencies.[171] This section does not cover the financial records of Internet users, which fall outside the current definition of financial institution.

C. *Access Affects Use*

The third offense covers access to computer used exclusively by or for the Government of the United States – where the access and conduct affects the use of the computer.[172] As in the previous section, the scope of this section is very narrowly drawn. The computer must belong to a department or agency of the United States, or the computer must be used by or for the Federal Government.[173] In *United States v. Morris*, an Internet user did affect the operation of Government computers, and this section applied.[174] However, this section does not cover unauthorized access to files of Internet users who fall outside this definition, such as corporations, businesses, academic institutions, and individuals.

D. *Computer Fraud*

The fourth offense is the first federal computer fraud statute. It criminalizes accessing a federal interest computer with intent to defraud and obtaining anything of value (other than computer time). A "federal interest computer" is defined as a computer:

> (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects the use of the financial institution's operation or the Government's operation of such computer; or

171. 18 U.S.C. § 1030(a)(2). Financial institutions, card issuers and consumer reporting agencies are defined as: an institution with deposits insured by the Federal Deposit Insurance Corporation, the Federal Reserve or a member of the Federal Reserve, a credit union insured by the National Credit Union Administration, a home loan bank, an institution under the Farm Credit System, a broker-dealer registered with the Securities Exchange Commission, the Securities Investor Protection Corporation, a branch or agency of a foreign bank, or an organization operating under § 25 or § 25(a) of the Federal Reserve Act. 18 U.S.C. § 1030(e)(4).

172. 18 U.S.C. § 1030(a)(3).

173. *Id.*

174. United States v. Morris, 928 F.2d 504 (2d Cir. 1991).

(B) which is one of two or more computers used in committing the offense, not all of which are located in the same state.[175]

An Internet user could fall within this section on either prong. However, it is more likely that the Internet user would fall within the second prong.

Many of the computers on the Internet are for government use or belong to financial institutions. If an Internet user accesses a Federal interest computer without authorization and with an intent to defraud, and the user obtains anything of value (other than computer time), the requirements for the first prong are satisfied. Alternatively, if routers[176] on the Internet are considered Federal interest computers, this section applies. However, routers typically contain no valuable information: all routers do is route messages. Therefore, one would not access an Internet router with intent to defraud, nor would one obtain anything of value from a router.

Nonetheless, section (B) of this act could apply. In fact, it could be presumed that a message sent on the Internet is routed interstate. Consequently, any use of the Internet is presumptively an interstate transaction. The intent of this definition was to aid local law enforcement officials when crimes were perpetrated across state lines. Prior to this change, the local law enforcement officials lost jurisdiction once the transaction traveled outside the state. However, with this provision, local law enforcement can enlist the aid of federal law enforcement officials who do have jurisdiction over interstate traffic.

What is unclear is if *any* Internet computer is a federal interest computer. If it is, then any access without authorization (or exceeding authorization) that furthers an intended fraud and obtains anything of value (other than computer time) falls within this section. Even if this broad definition is applied, however, the only crime covered by this section is fraud.

E. *Alters, Damages, or Destroys Information*

The fifth offense covers knowingly or recklessly altering, damaging, or destroying information.[177] Unlike the other subsections, which refer to a Federal interest computer, this section includes any "com-

175. 18 U.S.C. § 1030(e)(2).

176. A router in a message-switching system is the portion of a node or exchange that examines incoming messages, interprets the address information in each message and determines which of the ongoing links can be used. ROSENBERG, *supra* note 25, at 546. Routers, as used here, refers to any type of telecommunication device/computer which receives messages and routes them toward their destination. The term may include not only routers, but gateways, message switching computers, servers, etc.

177. 18 U.S.C. § 1030(a)(5).

puter used in interstate commerce or communication." Using this definition, any computer connected to the Internet would fall within the purview of this section. Since any computer accessing Internet engages in interstate communication, then any intentional access without authorization which alters, damages, or destroys information falls within this section. This subsection applies to any instance where the aggregate loss is greater than $1,000 in any one year or where there was any alteration or potential alteration to medical records.

F. *Trafficking Passwords*

The sixth offense deals with trafficking passwords.[178] This subsection is not limited to federal interest computers. Therefore, it applies to any Internet computer, as long as it could be shown that such trafficking affects interstate or foreign commerce, or is used by the U.S. government.

G. *Noncomputer Crimes*

Computer crimes, fraud, and password trafficking fall within the purview of the Act. However, noncomputer crimes do not. For example, pedophilia escaped liability under all six offenses:

1) A pedophile does not access national defense data, foreign relations data or data restricted by the Atomic Energy Act;
2) A pedophile does not access the financial records of a financial institution, card issuer or consumer reporting agency;
3) A pedophile does not access a computer of a department or agency of the United States used exclusively for the use of the Government;
4) A pedophile does not access the Internet with intent to defraud nor obtains any thing of value;
5) A pedophile does not alter, damage or destroy information;
6) A pedophile does not traffic passwords.

Pedophiles typically are authorized users, using a function for which they are authorized (*e.g.*, a bulletin board service or e-mail). Their use, per se, does not go outside the bounds of their authorization. Their use of the bulletin boards to stalk victims does not alter, modify, or destroy data, nor does it perpetrate a fraud resulting in pecuniary loss or theft of property. Therefore, pedophiles, or any criminal for that matter, can use the Internet to facilitate the perpetration of any crime – as long as they do not exceed their authorization, obtain anything of value, or use the Internet as an integral part of a fraud.

178. "Trading or dealing in certain goods . . . ." BLACK'S LAW DICTIONARY 1495 (6th ed. 1990).

Consequently, Congress (by starting ARPANET, which grew into the Internet)[179] has provided a low-cost and effective means for pedophiles to lure victims, child pornographers to distribute their obscene material, hatemongers to peddle their tracts, stalkers to locate their victims, and terrorists to distribute information on how to make and use explosives. Clearly this was not the intent of Congress.

IV. PROPOSED AMENDMENT TO THE ACT TO CRIMINALIZE TORTS AND NONCOMPUTER CRIMES

Modifying the Computer Fraud and Abuse Act was proposed in 1995 by Senator Leahy in the National Information Infrastructure Protection Act of 1995 (NIIPA).[180] Unfortunately, the NIIPA never emerged from the Judiciary Committee.[181] Congress apparently preferred the solution proposed by the Communications Decency Act,[182] which has just been found unconstitutional by a three-judge panel.[183]

The NIIPA would have extensively modified the Computer Fraud and Abuse Act. It would have included foreign communications.[184] It would have eliminated the duplicative language in subsection (a)(5)[185] and added liability for reckless damage.[186] It would have added extortion as a seventh offense.[187] Finally, it would have changed subsection (c), the punishment subsection, to incorporate punishments for the additional proposed offenses.[188]

One of the most interesting proposals in the NIIPA was the addition of language in subsection (c), the punishment section: "[I]f . . . the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." This language can serve as a model for criminalizing use of the Internet to commit noncomputer crimes. The wording of Senator Leahy's amendment has several advantages. It allows the current governmental agency (city, state or federal government) to continue to define and prosecute the underlying act. It makes it a federal offense to use the Internet to perpetrate a crime or tort, which in turns makes

179. *See supra* notes 8-16 and accompanying text.
180. S. 982, 104th Cong.; 1st Sess. (1995).
181. *Id.*
182. Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 133 (codified at 47 U.S.C. §§ 223, 230, 303, 330, 559, 640, 641; 18 U.S.C. §§ 1462, 1465, 2422).
183. ACLU v. Reno, No. 96-963, 1996 U.S. Dist. LEXIS 7919, at *205 (E.D. Pa. June 11, 1996).
184. S. 982 § 2(1)(B), 104th Cong.; 1st Sess. (1995).
185. *Id.* § 2(2)(B).
186. *Id.* § 2(1)(E).
187. *Id.* § 2(1)(F).
188. *Id.* § 2(2).

federal resources available to state and local governments. It creates additional penalties and provides the option of having the offender serve time in federal prison. By implementing this particular provision, the Computer Fraud and Abuse Act would address the current gap for noncomputer crimes.

The punishments for violation of this section could be fashioned similar to those of the other offenses. The fine could be "under this title"; the imprisonment could be set at the maximum of twenty years to allow the respective governments the optimal flexibility in determining additional incarceration:

> (c)(5) a fine under this title or imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(7).

These slight modifications to the Computer Fraud and Abuse Act would expand the scope of the Act to include noncomputer crimes. These modifications limit federal criminal liability to *use of the Internet* to perpetrate a crime or tort. It leaves to the respective federal, state, and local governments, the definition and prosecution of the underlying crimes. In addition, it makes only slight modifications to an existing act which has already undergone thorough review by the Department of Justice – as evidenced by the extensive modifications made to the Computer Fraud and Abuse Act in 1986.

CONCLUSION

The dark side of the Internet has grown to a critical mass. It has detonated a hue and cry that the federal government react to what has been classified in this comment as noncomputer crimes, *i.e.*, those crimes, such as pornography and pedophilia, which are not currently covered by the Computer Fraud and Abuse Act. While the Computer Fraud and Abuse Act has been amended several times, it still does not address the perpetration of noncomputer crimes.

Since cyberspace exists everywhere and nowhere at the same time, it is important that the control for defining and prosecuting noncomputer crimes remains where it currently resides – at the federal, state and local level, respectively. If this approach is not taken, there could be a tremendous federalization of crimes, and the local community would lose its ability to define and prosecute crimes based on local standards.

In response to these concerns, an amendment to the Computer Fraud and Abuse Act is proposed. It is based on a proposal by Senator Leahy in 1995. Punishment should be set at the maximum level to allow governments maximum flexibility in sentencing.

Making slight modifications to the Computer Fraud and Abuse Act, rather than creating new legislation, such as the Communications Decency Act,[189] has several advantages. It will minimize the amount of statutory analysis required. It will minimize the risk of the statute being found unconstitutional. It will allow law enforcement agencies to more quickly set about the task of cracking down on crimes perpetrated, or facilitated, by using the Internet.

189. *See supra* note 182 and accompanying text.